

[illegible]

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平10-31587

(43)公開日 平成10年(1998)2月3日

(51)Int.Cl. <sup>8</sup>	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 9/06	5 5 0		G 0 6 F 9/06	5 5 0 K
				5 5 0 E
15/00	3 3 0		15/00	3 3 0 Z

審査請求 未請求 請求項の数3 O L (全 7 頁)

(21)出願番号 特願平8-184406

(22)出願日 平成8年(1996)7月15日

(71)出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72)発明者 市毛 健志

神奈川県横浜市戸塚区吉田町292番地株式

会社日立製作所マルチメディアシステム開

発本部門

(74)代理人 弁理士 小川 勝男

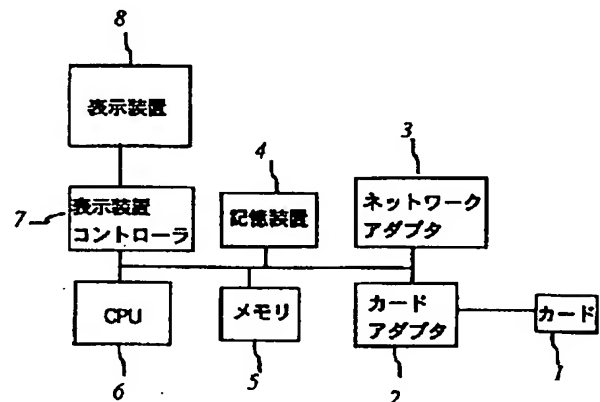
(54)【発明の名称】 データ端末装置およびコンピュータプログラム

(57)【要約】

【目的】 ネットワーク経由で配布するソフトウェアの使用権を遵守して動作するデータ端末装置を実現する。

【解決手段】 使用者の公開鍵で暗号化し、ソフトウェア開発元自らがデジタル署名したデータをソフトウェア使用権のためのデータとして、移動可能な媒体に記録し、データ端末装置はソフトウェア実行時にデータを読み出して使用権を検査し、検査結果に応じてその動作を変更する。

図 1



## DATA TERMINAL EQUIPMENT AND COMPUTER PROGRAM

Publication number: JP10031587

Publication date: 1998-02-03

Inventor: ICHIGE KENJI

Applicant: HITACHI LTD

Classification:

- International: G06F21/22; G06F9/06; G06F15/00; G06F21/00;  
G06F21/22; G06F9/06; G06F15/00; G06F21/00; (IPC1-7): G06F9/06; G06F15/00

- European:

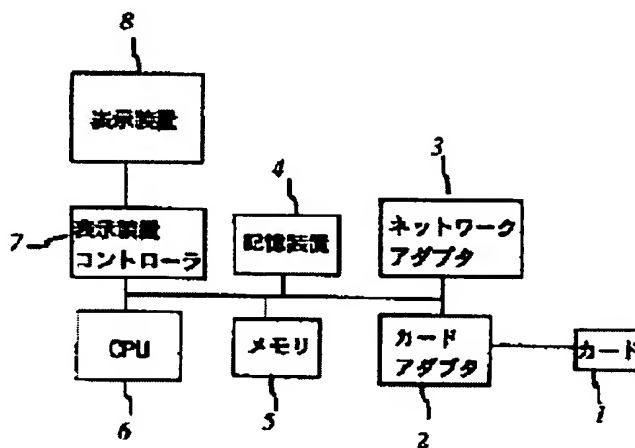
Application number: JP19960184406 19960715

Priority number(s): JP19960184406 19960715

Report a data error here

### Abstract of JP10031587

**PROBLEM TO BE SOLVED:** To prevent illegal use by ciphering data with the open key of a user, recording data which a software development source digitally signs in a movable medium, permitting a terminal equipment to read data and inspect use right and to change the operation in accordance with an inspected result at the time of executing software. **SOLUTION:** CPU 6 operates in accordance with basic software (OS) loaded on the memory 5 from a storage device 4 or a network adapter 3 and an application program and the processed result is displayed on a display device 8 through a display device controller 7. For operating the application program which the software development source develops, data which the software development source himself digitally signs is recorded in the memory 5 as data for software use right. The data terminal equipment reads data, inspects use right and changes the operation in accordance with the inspected result at the time of executing software.



Data supplied from the esp@cenet database - Worldwide

## 【特許請求の範囲】

【請求項1】 コンピュータプログラムを記録する記録手段と、上記記録手段より読み出した上記コンピュータプログラムを一時記憶するメモリ手段と、上記メモリ手段に記憶したコンピュータプログラムを実行する演算処理手段と、上記演算処理手段の処理結果を表示する表示装置と、外部ネットワークに接続するネットワーク接続手段と、脱着可能でかつ携帯可能な小型の脱着可能データ記憶手段と、上記脱着可能データ記憶手段を本装置に接続し、データを読み書きする脱着可能データ記憶接続手段より構成し、上記ネットワーク接続手段により上記外部ネットワークより上記コンピュータプログラムを読み込み、読み込んだ上記コンピュータプログラムは一時的に上記記憶手段に記憶するか、あるいは直接上記メモリ手段に記憶して上記演算処理手段により実行するようにし、上記脱着可能データ記憶手段には所有者の個々のコンピュータプログラムの使用権に関するデータを記憶し、上記コンピュータプログラムの実行時に上記使用権に関するデータを読み出して使用権の正当性を検査し、上記検査結果に応じて異なった動作をすることを特徴とするデータ端末装置。

【請求項2】 請求項1において、上記コンピュータプログラムの使用権に関するデータは上記コンピュータプログラムの著作権所有者により公開鍵暗号化方式に基づいて作成され、著作権所有者の秘密鍵および使用権購入者の公開鍵により暗号化されたデータであるデータ端末装置。

【請求項3】 請求項1において、上記コンピュータプログラムはその内部に上記脱着可能データ記憶手段に記憶された上記コンピュータプログラムの使用権に関するデータを検査するプログラムを含み、上記検査の結果に応じて処理動作を変更するようにプログラムしたコンピュータプログラム。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】 本発明はインターネット等の公共のネットワークにアクセスして動作するパソコン等のデータ端末装置およびその装置で実行するコンピュータプログラムに関する。

## 【0002】

【従来の技術】 従来のパソコン用ソフトウェアの入手方法について述べる。この入手方法は大きく二つの方法がある。第1の方法はユーザがパソコンショップへ出向き、店頭でパッケージングされたソフトウェアを購入する方法であり、第2の方法はネットワーク経由でソフトウェアをダウンロードして入手する方法である。ダウンロードとはネットワークで接続したホストコンピュータから自分のパソコン等に向かってのデータ通信によりソフトウェアをコピーすることである。

【0003】 第1の方法で購入したソフトウェアのパッ

ケージには、1) そのソフトウェアの実行形式のプログラムが記録してある記録メディア、通常はフロッピーディスクあるいはCD-ROM、2) 取扱説明書、3) ソフトウェア使用ライセンスを証明するシリアル番号(SN)、4) ソフトウェア使用ライセンス契約書等が梱包されている。ソフトウェア開発元とユーザ間のライセンス契約は記録メディア梱包を開封することにより成立するのが通常である。購入したソフトウェアを使用するためには、パソコン本体のハードディスク等の記録装置にソフトウェアの実行形式のプログラムをコピーしなければならない。この作業を一般的にインストール作業とよぶが、このインストール作業の方法はソフトウェアによって異なっている。単純に記録メディアに記録されているプログラムをコピーするだけでよいものもあれば、専用のプログラム(インストールプログラム)を実行してプログラムをコピーし、その際、シリアル番号を入力させユーザ毎に特価したプログラムをハードディスクにコピーする場合もある。あるいは、インストールの際に記録メディアにインストールを行ったことを示すデータを書き込むなどの動作をするインストールプログラムもある。シリアル番号の入力あるいは記録メディアの書換などは不正コピーの防止のためのものである。

【0004】 第2の入手方法では、記録メディアはない。取扱説明書、シリアル番号およびソフトウェア使用ライセンス契約書はデータの形で配布される。この方法の利点は簡単かつ迅速に広範囲にソフトウェアを配布できることである。第1の方法ではパッケージの箱を運送するなど流通コストがかかるが、第2の方法では構成要素はすべてのネットワーク上を伝送するだけでよい。第2の方法ではソフトウェアのアップグレードも迅速に行えるだけでなく、ソフトウェアの価格を低減することも可能である。しかし、この方法ではソフトウェアは容易に不正コピーができる欠点がある。インストールの過程でシリアル番号を入力させることでは十分な対策とはならない。

【0005】 近年のインターネットの普及によりだれでも容易にネットワークにアクセスして、ソフトウェアを入手することが可能になりつつある。ソフトウェア入手方法としては今後第2の方法が主流になると予想される。

【0006】 また、一方ではインターネットの普及に対応して、ネットワークに大きく依存して動作する新しい端末の形態が議論されている。この一例はオラクル社が1996年の自社の展示会で発表したネットワークコンピュータがある。これはネットワークアクセスを主たる目的とするものであり、500ドル程度の廉価な小型の端末装置で、少ない容量の記録装置に必要なソフトウェアのみを記録し、必要に応じてネットワークにアクセスしてソフトウェアをダウンロードしながら動作するものである。ユーザの個人情報および端末の動作条件等は付

10

20

30

40

50

属のICカードに記録し、ICカードを挿入し、パスワードを入力するだけで、個人認証を行い、ユーザの好みに応じた環境を構築して動作する。

#### 【0007】

【発明が解決しようとする課題】しかし、二つの入手方法のどちらを選んでもソフトウェアの不正使用を完全には防止することはできない。シリアル番号による不正使用防止策では不十分なのである。シリアル番号だけなら正規のライセンス取得者の知人であれば容易に聞き出すことが可能であり、ライセンスを正規に入手せずともソフトウェアを自分のハードディスクにインストールして使用することが可能である。

【0008】この不正使用防止策の不完全性は、ソフトウェア開発元にネットワーク経由でのソフトウェアの配布に対して消極的な態度をとらせる結果となる。

【0009】また、従来の方法によればソフトウェアの使用はインストールを行ったパソコンのみに限定されてしまう。ある時点で複数のパソコンにソフトウェアをインストールして使用することは許可されない。他のパソコンで同一のソフトを使用するためには、以前のパソコンにインストールしたソフトを専用のソフトウェアによるかあるいは単純に削除した後に、他のパソコンにインストールしなければならない。この制限は通常ソフトウェア使用ライセンス契約書に明記されている規約事項であるが、本来購入したのはソフトウェアの使用ライセンスであるのだからライセンスを取得したものならばどのパソコンでも当のソフトウェアが使えることが望ましい。

【0010】特にネットワーク依存型の端末では頻繁にネットワークにアクセスして、ソフトウェアをダウンロードするが、ネットワークの効率的使用のためにはソフトウェアを分散して配置してデータトラフィックの集中をさせないようにすることが望ましい。このためには適切な不正使用の検査システムが必要であるが、その動作に際してもソフトウェア開発元へのデータの集中を避けなければならない。

【0011】シリアル番号の盗用による不正使用を摘発するための方法として、ソフトウェアの動作時にシリアル番号をネットワーク経由でソフトウェア開発元に集めて検査することが考えられるが、この方法はソフトウェア開発元にデータを集中されるものであり好ましくない。

【0012】本発明の第1の目的は、ソフトウェアをネットワーク経由でパソコン等のネットワーク端末にダウンロードし、ソフトウェアを動作させる際に、ソフトウェアの使用ライセンス契約が正しく守られているかチェックし、不正使用を防止するシステムを提供することである。ただし、このシステムの運用がネットワーク経由でのソフトウェアの配布を促進する方向に働かねばならない。また、システムがその運用により極端にホスト側

へのデータの集中を起こすものではない。

【0013】本発明の第2の目的はソフトウェア使用ライセンスを端末から切り離し、どの端末でも使用ライセンスを取得したソフトウェアを使用可能にすることである。

#### 【0014】

【課題を解決するための手段】この課題を解決するためソフトウェアライセンスをデータ化し、移動可能な媒体に記録し、ソフトウェア使用時にデータを読み出してライセンスを検査する。

【0015】データ化のために公開鍵暗号化方式を用い、ソフトウェア開発元が使用者の公開鍵で暗号化し、かつソフトウェア開発元自らがデジタル署名したデータをソフトウェアライセンスのためのデータとする。

【0016】ソフトウェアは実行時に移動可能な媒体からデータ読み出し、データを復号することを試みる。データが正当なものでなければ、復号化は失敗して適当な復号化データを得ることができず、ソフトウェア使用ライセンスが正しく取得されていないことを知ることができる。ソフトウェアは検査結果に基づいてソフトウェアの機能を制限あるいは変更して動作する。

#### 【0017】

【発明の実施の形態】以下、図面を用いて本発明の実施例を説明する。

【0018】図1は本発明の第1の実施例であり、インターネットなどのネットワークにアクセスしてソフトウェアをダウンロードし、ダウンロードしたソフトウェアを実行する装置本体の構成を示す。1は移動可能な記録媒体（カード）、2はカード1を読み書きするための記録・読みだし装置（カードアダプタ）、3はネットワークとの間でデータあるいはプログラムを送受信するネットワークアダプタ、4はハードディスクなどのソフトウェアおよびデータを記録するための記録装置、5はメモリ、6はCPU（Central Processor Unit; 中央演算処理ユニット）、7は表示装置コントローラ、8は表示装置、9はキーボード・マウスなどの入力装置である。カード1、カードアダプタ2を除くと通常のパソコンと基本的には同様の構成である。

【0019】CPUは記憶装置4あるいはネットワークアダプタ3より基本ソフト（OS）とアプリケーションプログラムをメモリ5にロードする。OSおよびアプリケーションプログラムはCPUに対する命令およびその他のデータにより構成されるものであり、CPUはメモリにロードしたOSおよびアプリケーションプログラムにしたがって動作する。OSおよびアプリケーションプログラムを総称して単にプログラムと記す。記憶装置4には使用頻度の高い全部あるいは必要な部分のプログラムを記録しておき、動作時に生じるプログラムの不足分はネットワークアダプタ3を使用してネットワークよりコピーしてメモリ5にロードする。CPUの処理結果は

表示装置コントローラ7を経由して、表示装置8に送る。利用者は表示装置8を見ることにより、プログラムの動作結果を知ることができる。利用者からの指示は入力装置9よりCPUに伝達される。

【0020】カード1はカードアダプタ2に対して容易に何度でも抜き差し可能なものであり、CPU6はカードアダプタ2に挿入したカード1のデータ内容を読み書きすることができる。このカードとしてICカード、フロッピーディスクなどのメディアを使用することができる。

【0021】図3は動作時のメモリ5の内容を示したものである。ここではユーザBが本装置を用いてソフトウェア開発元Aが開発したアプリケーションプログラムP1を動作させる場合を説明する。ユーザBは正規にP1の使用ライセンスを取得しているとする。OSおよびアプリケーションプログラムのプログラムサイズがメモリ5の容量に対して十分に小さいならばそれらプログラムのすべてのプログラムコードをメモリ5にロードする。そうでなければ、メモリ5にはOSおよびアプリケーションプログラムのプログラムコードの内の必要部分あるいは使用頻度の高い部分のみを常駐させる。動作時に不足分が生じた場合、プログラムの不足分は記録装置4からメモリ5にロードするかあるいはネットワークアダプタ3を使用してネットワークよりコピーしてメモリ5にロードする。いずれにしる動作時にはOSおよびアプリケーションプログラムの一部あるいは全部がメモリ5にロードされる。

【0022】アプリケーションプログラムP1の動作の初期段階で使用ライセンスの検査を行う。このため、この段階ではP1のプログラム領域にはP1を識別するためのコードであるプログラムコードPID、ライセンス検査プログラム、A社の公開鍵PKA、ライセンス検査プログラムがロードされ、OSのプログラム領域には公開鍵暗号化プログラムと記録媒体読み書きプログラムがロードされている。

【0023】ここで、PIDはプログラムP1を識別するためのコードである。プログラム名あるいはプログラム毎にユニークに決められた数字などを用いる。処理を簡単にするためには所定サイズのデータにすることが望ましい。

【0024】ライセンス検査プログラムはP1の使用ライセンスをユーザが正規に取得しているかを検査するプログラムである。ユーザBのライセンスに関するデータはカード1に記録されているので、このデータを読み出すために記録媒体読み書きプログラム303を呼び出して実行する。さらに、このデータを復号するために公開暗号化プログラム302を呼び出して実行する。

【0025】図2はカード1に記録したデータ内容を示すものである。データ内容は所有者の公開鍵および秘密鍵、認証者の公開鍵、ライセンス管理テーブル、個々の

ライセンスデータより構成する。公開鍵および秘密鍵は公開暗号化方式の暗号化あるいは復号化で使用する鍵データであり、所有者の公開鍵は適当な認証者たとえば銀行あるいは公共機関などにより認証を受けたものを用いる必要がある。公開鍵の正当性を高めるため、認証者は複数であることが望ましい。ライセンス管理テーブルは複数のライセンスデータを管理するためのデータであり、図に示すように全ライセンス数、個々のライセンスデータの対応するプログラムのPID、カード内での記憶位置、サイズより構成する。ライセンスデータはユーザの個々のソフトウェアに対するソフトウェア使用ライセンスをデータ化したものである。

【0026】ライセンスデータはソフトウェア開発元が特定のユーザに対して該当するソフトウェアの使用ライセンスを証明するものである。具体的には、ソフトウェア開発元がユーザよりユーザの公開鍵を入手し、該当するソフトウェアが使用するデータをユーザの公開鍵により公開鍵暗号化し、暗号化したデータをソフトウェア開発元の秘密鍵により公開鍵暗号化した暗号化データあるいは同様の暗号化データをソフトウェア開発元がデジタル署名した暗号化データを用いる。ユーザの公開鍵により暗号化することにより、ユーザ以外には現実的には復元不可能なデータとなり、ユーザのみがそのライセンスデータを使用することが可能になる。ここで、現実的と限定を加えた理由は、公開鍵暗号化方式により暗号化した暗号化データを復号化の鍵の所有者以外のものが復元することは不可能とは言えないが、そのためには非現実的なほど膨大な時間あるいは費用が発生するのでできないとの意図である。以降の説明ではそのような場合には現実的の限定なしに述べることにする。また、ライセンスデータ生成の最後の過程がソフトウェア開発元のデジタル署名でも暗号化でもよい理由は、どちらによってもソフトウェア開発元によって作成されたデータであることが証明されるからである。説明でユーザおよびソフトウェア開発元の秘密鍵は正しく管理され、第3者がそれを使用できない状態にあることは前提条件である。また、ユーザおよびソフトウェア開発元の公開鍵は少なくとも一つ以上の共通の認証者によって承認されていることが、相互の公開鍵の正当性の確認のために必要である。

【0027】説明でソフトウェアが必要とするデータとは、ソフトウェア毎にその数、内容が異なってよい。そのデータはソフトウェアの動作に変化させることもあれば、その動作にはまったく無関係のデータでもよい。

【0028】最も単純な場合の例として、データとしてソフトウェアのシリアル番号(SN)を用いることを考えることができる。これは数1により示すことができる。

【0029】

【数1】

7

プログラムP1のユーザBに対するライセンスデータL1:

$$L1 = ((SN1 * SKA) * PKB) \quad \dots \text{〔数 1〕}$$

ただし、

\*: 公開鍵暗号化演算、

SN1: ユーザBに割り当てられたプログラムP1のSN、

SKA: A社の秘密鍵、

PKB: Bの公開鍵。

【0030】

\* \* 〔数 2〕

プログラムP1のユーザBに対するライセンスデータL1:

$$L1 = (((SN1+X) * SKA) * PKB) \quad \dots \text{〔数 2〕}$$

ただし、

\*: 公開鍵暗号化演算、

SN1: ユーザBに割り当てられたプログラムP1のSN、

X: プログラムの動作を変化させるパラメータ、

SKA: A社の秘密鍵、

PKB: Bの公開鍵。

【0031】ここでライセンスデータはL1、ユーザBの公開鍵はPKB、ソフトウェア開発元Aの秘密鍵はSKA、プログラムP1のSNはSN1、公開暗号化方式による暗号化演算は記号\*で表わす。ソフトウェア開発元Aは数2に基づきライセンスデータL1を発行し、ネットワーク経由でユーザBに送信する。ユーザB以外の者はライセンスデータL1を利用不可能なデータであり、第3者に盗聴あるいはコピーされたとしても問題は起らない。

【0032】前述の例より複雑な例としては、この例のSNに替えて、ソフトウェアの動作条件を決定するパラメータ、付加機能使用許可のためのデータ、使用期間を限定するデータなどを使用することが考えられる。ソフトウェアの動作条件を決定するパラメータの例は各国語へのローカライズのデータが考えられる。地球規模のグローバルなネットワーク上を同一のソフトウェアを配布し、動作時に各国語に応じて切り替えるだけでよい場合に対応する。付加機能使用許可のためのデータの例は、ソフトウェアの機能として一般のユーザは使用しない専門的な機能をオプションとして加える場合が考えられる。この場合、当然ながらライセンス料などの契約条件が変わることが予想される。使用期間限定のデータの例は、ソフトウェアの試用が考えられる。ソフトウェアの新規ユーザ獲得のために一定期間に限り無償で試用を許可することは有効である。この場合でも、ソフトウェア本体は正規ユーザのものと同一のものを使用することができる。この様にライセンスデータを変えることにより、同一のソフトウェアを配布しながら、個々のライセンス契約の内容に応じた動作をさせることが可能である。

【0033】ソフトウェアの動作の過程を図5のフローチャートで説明する。ソフトウェアP1は記録装置あるいはネットワークアダプタよりメモリロードされた後実行される。ロード直後にソフトウェアP1内部のライセ

ンス検査プログラムが実行される。このライセンス検査プログラムはカード1より対応するライセンスデータを読み出し検査する。検査結果を条件として分岐して、各結果毎(結果1、結果2、…、結果k)の処理(処理1、処理2、…、処理k)を行う。ここで、分岐の数kはプログラムに依存する数で通常2以上である。結果の中のどれかは不正なライセンスを使用した場合に対応する。

【0034】本実施例によれば、ソフトウェアをネットワーク経由で配布する際にもライセンスを正しく管理することができ、不正使用を防止することができる。また、使用ライセンスをデータ化し、データにソフトウェア使用上の条件を内包することにより、同一のプログラムを配布しておきながらユーザ毎のライセンスの内容に応じた動作をするプログラムを提供することができる。

【0035】

【発明の効果】本発明によればネットワーク経由で配布するソフトウェアの使用ライセンスの管理を正しく行うことができるので、ソフトウェア開発元は安心して有償のソフトウェアのネットワーク経由で出荷することができる。これによりソフトウェアのアップグレードが行われる際には世界中場所を問わず迅速なアップグレードを行うことができる。また、ネットワークによる配布による流通コストの低減、および不正コピー防止の効果により、ソフトウェア代金の低価格化に効果がある。

【図面の簡単な説明】

【図1】第1の実施例を示すブロック図。

【図2】第1の実施例における記録媒体のデータ内容を示す説明図。

【図3】第1の実施例におけるソフトウェア動作時のメモリ内容を示す説明図。

【図4】第1の実施例の装置の利用形態を示すブロック図。

【図5】第1の実施例のアプリケーションプログラムの

8

50

動作フローチャート。

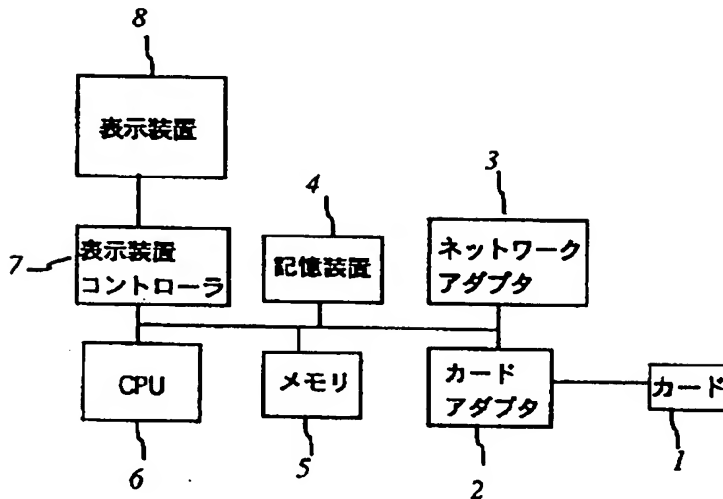
【符号の説明】

- 1…移動可能な記録媒体、  
2…記録媒体の記録・読み出し装置、  
3…ネットワークアダプタ、

- \* 4…本体の記録装置、  
5…メモリ、  
6…CPU、  
7…表示装置コントローラ、  
\* 8…表示装置。

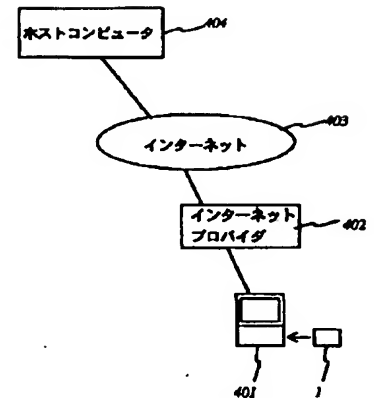
【図1】

図1



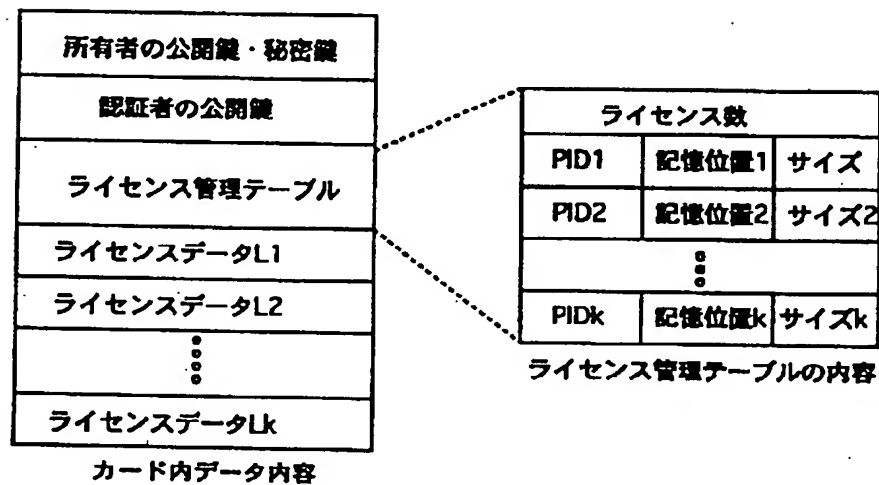
【図4】

図4



【図2】

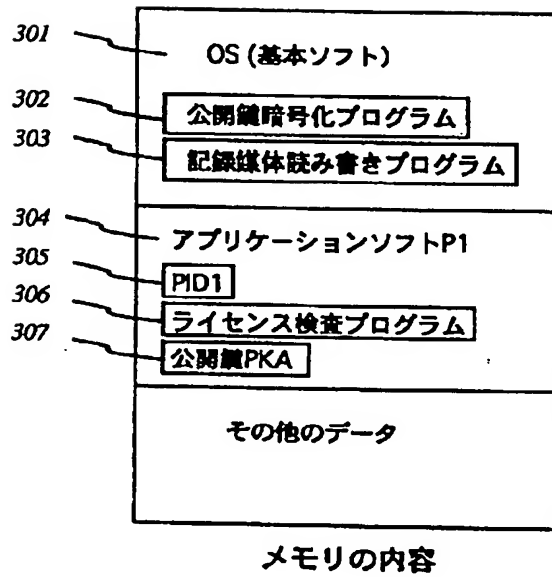
図2





【図3】

図3



【図5】

図5

